What is claimed is:

1. A computing system being a first computing system connected with a second computing system by a communication channel, wherein:

said first computing system receives encrypted data from said second computing system, and stores said encrypted data without decrypting.

2. A computing system being a first computing system connected with a second computing system by a communication channel, wherein:

said first computing system has a storage system, receives encrypted data from said second computing system, and stores said encrypted data without decrypting in said storage system.

3. The computing system recited in Claim 2, wherein:

said first computing system has a network connection device, receives a cryptographic key and encrypted data from said second computing system, and stores said encrypted data without decrypting in said storage system.

4. The computing system recited in Claim 2, wherein:

said first computing system has a processor system, receives a cryptographic key and encrypted data from said second computing system, and stores said encrypted data without decrypting in said storage system.

5. The computing system recited in Claim 2, wherein:

said processor system reads encrypted data from said storage system, decrypts it, and further writes it in said storage system.

6. The computing system recited in Claim 2, wherein:

said network connection device reads encrypted data from said storage system,

decrypts it, and further writes it in said storage system.

7. The computing system recited in Claim 2, wherein:

said storage system reads encrypted data within said storage system itself, and decrypts and writes it.

8. The computing system recited in Claim 2, wherein:

said first computing system has a decryption device, said decryption device reads encrypted data from said storage system, decrypts it, and further writes it in said storage system.

9. The computing system recited in Claim 5, wherein:

reading of encrypted data from said storage system and writing of decrypted data are performed with respect to the same storage position in said storage system.

10. The computing system recited in Claim 5, wherein:

received encrypted data is stored in sequence of receipt without decryption in said storage system, and reading of encrypted data from said storage system and writing of decrypted data are such that writing is to a position being different from the position read in said storage system.

11. The computing system recited in Claim 5, wherein:

the interval of reading of encrypted data in said first computing system is an interval of fixed time.

12. The computing system recited in Claim 5, wherein:

reading of encrypted data in said first computing system is started by request from the storage system in said first computing system.

13. The computing system recited in Claim 5, wherein:

an encryption key is received from the storage system in said first computing system.

14. The computing system recited in Claim 5, wherein:

an encryption key is received from the network connection device in said first computing system.

15. The computing system recited in Claim 5, wherein:

an encryption key is received from the processor system in said first computing system.

16. An encryption and decryption method comprising the steps of:

reading encrypted data from a storage system that stores encrypted data received in a computing system without decrypting;

decrypting it; and

further writing it to said storage system.

17. An encryption and decryption method comprising the steps of:

passing a cryptographic key to a decryption device from a storage system that stores the cryptographic key and encrypted data which is not decrypted, received in a computing system;

sequentially sending said received encrypted data to said decryption device;

decrypting it; and

further writing it from said decryption device to said storage system.

18. A computer system with remote copy facility comprising:

a main center consisting of a primary disk subsystem group having a control means that is connected to an upper layer device and performs sending and receiving of data and a storage means that performs storage of said data; and

a remote center, which is disposed in a place apart from said primary disk subsystem

group, consisting of a secondary disk subsystem group having a control means and receives encrypted data transferred from said primary disk subsystem group and a storage means that performs storage of said transferred data,

wherein said primary disk subsystem group updates a cryptographic key at a specified interval or an irregular interval, also interrupts said data transfer to said secondary disk subsystem group and transfers the updated cryptographic key to said secondary disk subsystem group.

19. The computer system with remote copy facility recited in Claim 18, wherein:

said primary disk subsystem group creates data having the same data length and data pattern as data transferred to said secondary disk subsystem group, and embeds said cryptographic key in said created data.

20. A computer system with remote copy facility comprising:

a main center consisting of a primary disk subsystem group having a control means that is connected to an upper layer device and performs sending and receiving of data and a storage means that performs storage of said data; and

a remote center, which is disposed in a place apart from said primary disk subsystem group, consisting of a secondary disk subsystem group having a control means and receives encrypted data transferred from said primary disk subsystem group and a storage means that performs storage of said transferred data,

wherein said primary disk subsystem group, during execution of data write processing, determines whether or not it is time for updating the cryptographic key for encrypted data transfer, and if it is time for updating, updates said cryptographic key, also transfers it to said secondary subsystem assigning a sequence number to said updated cryptographic key, and

associates it with the transferred data assigned with the sequence number.

21. The computer system with remote copy facility recited in Claim 18, wherein:

data encrypted and transferred from said primary disk subsystem group to said secondary disk subsystem group is kept without decrypting in the storage means of said remote center, and is decrypted in time of disaster recovery.

22. The computer system with remote copy facility recited in Claim 21, wherein:

when data is encrypted and transferred from said primary disk subsystem group to said secondary disk subsystem group, said cryptographic key is remote copied to and kept at another remote center disposed in a place separate from said remote center, and data is decrypted using the cryptographic key kept at said other remote center in time of disaster recovery.

23. An encryption system of the computer system with remote copy facility recited in Claim 21, wherein:

when data encrypted and transferred from said primary disk subsystem group to said secondary disk subsystem group is decrypted, it is decrypted only when a specific portion of a record concerning said data was searched.

24. The computer system with remote copy facility recited in Claim 18, wherein:

said primary disk subsystem group and said secondary disk subsystem group are connected via a storage area network.

25. The computer system with remote copy facility recited in Claim 18, wherein:

data transfer between said primary disk subsystem group and said secondary disk subsystem group is performed by synchronous transfer or asynchronous transfer.

26. A computer system with remote copy facility comprising:

a main center consisting of a primary disk subsystem group being connected to an upper layer device and receiving data transfer from said upper layer device; and

a remote center consisting of a secondary disk subsystem group being connected with said primary disk subsystem group of said main center and receiving data transfer,

wherein said primary disk subsystem group has a remote copy control information storage component that stores control information stipulating whether or not encrypted data transfer is performed when remote copying data to said secondary disk subsystem group, and performs data encryption when said control information stipulates to perform encrypted data transfer; and

said secondary disk subsystem group confirms said control information of said primary disk subsystem group, and performs processing appropriate to the encryption with respect to the transferred data when said control information is to perform encrypted data transfer.

27. A remote copy method of a storage system comprising:

a local storage system that stores data written from an upper layer device; and

a remote storage system that stores a copy of said data, wherein comprising:

a step where said local storage system encrypts said data with a cryptographic key;

a step where said encrypted data is transferred from said local storage system to said remote storage system;

a step where said cryptographic key is iteratively updated; and

a step where said updated cryptographic key is transferred from said local storage system to said remote storage system,

wherein said encryption step uses the updated cryptographic key after said cryptographic key was updated.

28. The remote copy method of the storage system recited in Claim 27, wherein:

the frequency of iteration of the step where said cryptographic key is updated is determined from the time for deciphering said cryptographic key.

Abstract of the Disclosure

Providing a computing system and encryption/decryption method that realizes assurance of security and improvement of throughput in a remote system.

There are provided a means that writes encrypted data to a storage system, a means that identifies whether data in the storage system is ciphertext or plaintext, and a means that reads, decrypts, and rewrites encrypted data in storage asynchronously with writing encrypted data to storage.